AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated hereafter (where underlining "_" denotes additions and strikethrough "-" denotes deletions).

Claims:

1.   (Previously Presented)   A method for providing automated diagnosis of problems for a computer network, comprising:

    identifying recent configuration changes made to the computer network that fall within pre-established parameters;

    ranking the identified changes into potential causes;

    verifying ranked potential causes to determine whether any of the ranked potential causes may be an actual cause or contributor to the problem; and

    calculating distances associated with the ranked potential causes that correspond to a relative likelihood that potential causes may be a true cause.

2.   (Original)   The method of claim 1, further comprising formulating a list of possible causes based on or ordered in terms of the distances and presenting the list to a user.

3.   (Original)   The method of claim 1, further comprising discarding the ranked potential causes that violate a configurable distance threshold.

4.   (Original)   The method of claim 1, further comprising recording policy or configuration changes that occur.

5.   (Original)   The method of claim 1, further comprising accumulating and ranking potential causes until all potential causes associated with the problem are received.

6.   (Original)   The method of claim 1, further comprising searching a database having user records, vulnerability and reliability data to verify the potential causes.

7.   (Previously Presented)   The method of claim 1, further comprising interpreting the computer network's policies as needed to complete the verifying step.

8.   (Previously Presented)   A computer-readable medium executable on a computer having a program for providing automated diagnosis of problems for a computer network, for performing the steps of:

      logic configured to identify recent configuration changes made to the computer network that fall within pre-established parameters;

      logic configured to rank the identified changes into potential causes;

      logic configured to verify ranked potential causes to determine whether any of the ranked potential causes may be an actual cause or contributor to the problem; and

      logic configured to calculate distances associated with the ranked potential causes that correspond to a relative likelihood that potential causes may be a true cause.

9.   (Original)   The computer-readable medium of claim 8, further comprising logic configured to formulate a list of possible causes based on the distances and logic configured to present the list to a user.

10.   (Original)   The computer-readable medium of claim 8, further comprising logic configured to discard the ranked potential causes that violate a configurable distance threshold.

11.   (Original)   The computer-readable medium of claim 8, further comprising logic configured to record policy or configuration changes that occur.

12.   (Original)   The computer-readable medium of claim 8, further comprising logic configured to accumulate and rank the potential causes until all potential causes associated with the problem are received.

13.   (Original)   The computer-readable medium of claim 8, further comprising logic configured to search a database having user records, vulnerability and reliability data to verify the potential causes.

14.   (Previously Presented)   A system for providing automated diagnosis of problems for a computer network, comprising:

      a central diagnosis engine configured to include:

            a rank estimator module configured to rank identified changes into potential causes;

            a verifier module configured to verify ranked potential causes to determine whether any of the ranked potential causes may be an actual cause or contributor to the problem; and

            a distance estimator module configured to calculate distances associated with the ranked potential causes that correspond to a relative likelihood that potential causes may be a true cause; and

      an adaptive logger operative coupled to the central diagnosis engine, the adaptive logger is configured to record policy or configuration changes made to the computer network that fall within pre-established parameters.

15.   (Original)   The system of claim 14, further comprising an input parser/filter module operatively coupled to the central diagnosis engine, the input parser/filter including logic configured to receive policy or profile input from a user's processing device or policy-management systems and to convert the input into data usable by the central diagnosis engine.

16.   (Original)   The system of claim 14, further comprising an input parser/filter module operatively coupled to the central diagnosis engine, the input parser/filter including logic configured to receive a problem indication and descriptive information from sensor and monitoring systems and to convert that input into data usable by the central diagnosis engine.

17.   (Original)   The system of claim 15, further comprising a database populated with descriptive system information and a database structure configured as hierarchical database pages, each database page having a page index, data section and selector section, and wherein the data section is further configured to include the element reliability or vulnerability information and the selector section is further configured to include links to related database pages.

18.   (Original)   The system of claim 17, wherein the central diagnosis engine further comprises a problem accumulator module configured to receive problem data from the input parser/filter module and to continue receive data until the problem is fully described.

19.   (Original)   The system of claim 18, wherein the central diagnosis engine further comprises a cause estimator module configured to interface with the adaptive logger and to identify any changes in policy or configuration associated with any available parameters of the problem.

20.   (Original)   The system of claim 19, wherein the central diagnosis engine further comprises a possible cause accumulator module configured to receive and accumulate potential causes and rankings from the rank estimator module until the ranking is complete and potential causes associated with the problem are received.

21.   (Previously Presented)   The system of claim 20, wherein the central diagnosis engine further comprises a policy interpreter module configured to provide details on the computer network's configuration to the verifier module as needed in the verification process.

22.   (Original)   The system of claim 21, further comprising a presentation module operatively coupled to the central diagnosis engine and a user's processing device through a communications network, the presentation module configured to summarize and format at least one of accumulated possible causes, distances, probabilities, related reliability or vulnerability results for utilization by the user's processing device.

23.   (Original)   The system of claim 22, further comprising a database interface module operatively coupled between the database, the database structure, and the central diagnosis engine, the database interface module configured to enable provisioning and access to the database and the database structure.

24.   (Original)   The system of claim 23, wherein the database comprises an element descriptive database (EDD).

25.   (Original)   The system of claim 24, wherein the database structure comprises a hierarchical vulnerability database (HVD) structure.